GUID 5100

Упатство за ревизија на информациски системи

Упатствата на INTOSAI се издаваат од Меѓународната организација на врховни ревизорски институции, INTOSAI, како дел од Рамката за професионални објави на INTOSAI. За повеќе информации посетете ја www.issai.org

INTOSAI

INTOSAI

INTOSAI, 2019 година

1) Одобрен во 2016 година, како ISSAI 5100 – Упатство за ИТ ревизија.
2) Преквалификуван и преименуван во GUID 5100 – Упатство за ревизија на информациски системи во 2019 година

СОДРЖИНА

1. ВОВЕД 4

2. ЦЕЛ НА ОВА УПАТСТВО 6

3. ДЕФИНИЦИИ 7

4. ОПФАТ 8

5. ПЛАНИРАЊЕ НА РЕВИЗИЈА НА ИС 9

6. ИЗВРШУВАЊЕ НА РЕВИЗИЈА НА ИС 14

7. ИЗВЕСТУВАЊЕ ЗА РЕВИЗИЈАТА НА ИС 19

8. FOLLOW UP 20

1

ВОВЕД

1.1 GUID 5100 ја обезбедува главната рамка за спроведување на ревизија на информациските системи во Рамката за професионални објави на INTOSAI (IFPP). Ова Упатство е наменето да обезбеди основа за развој на идни упатства во серијата 5100-5109 за предметната област на ревизијата на информациските системи во Рамката за професионални објави на INTOSAI (IFPP).

1.2 Рамката утврдена со ова Упатство е во согласност со *Основните принципи на ревизија на јавниот сектор* (ISSAI 100), *основните принципи на финансиска ревизија* (ISSAI 200), *Принципите на ревизијата на успешност* (ISSAI 300) и *Принципите на ревизијата на усогласеност* (ISSAI 400).

1.3 Врховните ревизорски институции (ВРИ) имаат мандат да вршат ревизија на владите и нивните субјекти согласно нивните ревизорски мандати[1]. Преку своите активности, ВРИ имаат за цел да промовираат ефикасност, отчетност, ефективност и транспарентност на јавната администрација[2].

1.4 Владите и другите субјекти од јавниот сектор континуирано прифаќаат новини од областа на информатичката технологија (ИТ) во нивните информациски системи, со цел да се подобри ефикасноста и ефективноста во нивното функционирање и испорака на разни јавни услуги. Ова е поради тоа што ИТ овозможува електронско снимање, складирање, обработка, преземање и испорака на информации, што, пак, создава значителен опфат за подобрување на мерилата за точност, доверливост и навременост на информациските системи. Покрај тоа, начинот на испорака на јавните услуги брзо преминува од физички во електронски, што резултира со трансформација на функционирањето на владите во дигитални платформи кои обезбедуваат услуги, како и со инфраструктура за други информациски системи управувани од ИТ.

[1] INTOSAI-P 1 Декларација од Лима

[2] Резолуција на Генералното собрание на ОН A/66/209

15 Оваа транзиција кон компјутеризирани информациски системи и електронска обработка на субјектите на ревизија во јавниот сектор предизвика значителна промена во опкружувањето на ВРИ. Расходите на јавниот сектор за ИТ растат. Исто така, постои потреба од потврда дека внатрешните ИТ контроли за одржување доверливост, интегритет и достапност на податоците се усвоени од субјектите во јавниот сектор. Од овие причини, развивањето на соодветни капацитети за вршење темелно испитување на контролите поврзани со информациските системи станува императив за ВРИ.

2

ЦЕЛ НА ОВА УПАТСТВО

2.1 ISSAI 100, 200, 300 и 400 ги утврдуваат основните ревизорски начела на финансиската ревизија, ревизијата на успешност и ревизијата на усогласеност. Овие ISSAI се однесуваат на општите принципи, процедури, стандарди и очекувања од ревизорот. Тие се подеднакво применливи и за ревизијата на информациските системи.

2.2 Целта на ова Упатство е да обезбеди насоки за ревизорите како да спроведат ревизии на успешност и/или усогласеност поврзани со одредена тема за информациските системи или каде што ревизијата на информациските системи може да биде дел од поголем ревизорски ангажман како финансиска ревизија, ревизија на усогласеност или ревизија на успешност.

2.3 Содржината на ова Упатство може да ја применуваат ревизорите во фазите на планирање, спроведување, известување и следење на процесот на ревизија[3].

[3] ISSAI 100

3

ДЕФИНИЦИИ

3.1 Информациските системи може да се дефинираат како комбинација на стратешки, менаџерски и оперативни активности вклучени во прибирање, обработка, складирање, дистрибуција и користење на информациите и сродните технологии. Комплексноста на еден ваков информациски систем може да варира од едноставна книга во која рачно се водат записи за примање и плаќање пари, до покомплексен ИТ управуван систем, како што е системот за проценка на данок, во кој сите процеси – прибирање на податоци (на пр. даночни пријави поднесени преку онлајн веб-портал), складирање на сервери, обработка на проценка (заснована на програмирање, користејќи правила за оданочување) и информирање за оданочување, поврат и признавање на данок (во реално време или во пропишани интервали) се автоматизирани. Информатичката технологија се состои од хардвер, софтвер, комуникација и други уреди што се користат за внесување, складирање, обработка, пренесување и излез на податоци во било каква форма.

3.2 Ревизија на информациските системи може да се дефинира како испитување на контролите поврзани со ИТ управувани информациски системи, со цел да се идентификуваат случаи на отстапување од критериумите кои, пак, се идентификувани врз основа на видот на ревизорскиот ангажман - т.е. финансиска ревизија, ревизија на усогласеност или ревизија на успешност.

4

ОПФАТ

4.1 Ова Упатство може да го користат ревизорите при вршење ревизии на успешност и/или усогласеност на одреден предмет во врска со информациските системи, како и во случаи кога ревизијата на информациските системи е дел од поголем ревизорски ангажман како финансиска ревизија, ревизија на усогласеност или ревизија на успешност.

4.2 Ова Упатство дава дополнителни насоки за тоа како може да се пристапи на секоја ревизија на информациските системи со спроведување на финансиска ревизија / ревизија на успешност / ревизија на усогласеност и не содржи други барања за спроведување на ревизијата.

5

Планирање на ревизија на информациски систем (ИС)

5.1 ВРИ можат да усвојат планирање на ревизијата базирано на ризици за ревизии на ИС, во согласност со процесот опишан во ISSAI 100, ISSAI 200 (финансиска ревизија), ISSAI 300 (ревизија на успешност) и ISSAI 400 (ревизија на усогласеност), во зависност од целите на ревизорскиот ангажман.

5.2 Ревизорската работа на ИС ќе биде одредена согласно целта и опфатот на ревизијата, како на пример:

1) Да се оценат релевантните општи контроли[4] и апликациски контроли[5] кои влијаат на веродостојноста на податоците од информациските системи, кои, пак, влијаат на финансиските извештаи на субјектот на ревизија.
2) Да се добие уверување за усогласеноста на процесите на информациските системи со законите, политиките и стандардите што се применуваат на субјектот на ревизија.
3) Да се добие уверување дека ИТ ресурсите овозможуваат ефикасно и ефективно постигнување на организациските цели и дека релевантните општи контроли и апликациски контроли се ефективни во спречување, откривање и корекција на случаи на вишок, екстраваганција и неефикасност во користењето и управувањето со информациските системи.

5.3 Врз основа на проценка на ризик, опфатот на ревизијата на ИС може да се извлече од една или од сите следни области[6] на субјектот на ревизија:

[4] Општи контроли се мануелни или автоматизирани процедури кои имаат за цел да осигурат доверливост, интегритет и достапност на информациите во физичкото опкружување во кое се развиваат, одржуваат и работат информациските системи

[5] Апликациски контроли се ИТ зависни мануелни или автоматизирани процедури во рамките на информациски систем кои влијаат на обработката на трансакциите и може да се однесуваат на валидација на влезни податоци, точна обработка на податоци, испорака на излезни податоци и контроли поврзани со интегритетот на матичните податоци

[6] Повеќето од опишаните домени се адаптирани според ISO / IEC 27001

1) Организациска политика за ИТ[7]
2) Структура на организациско управување на тема ИТ
3) Автоматизирани општи контроли обезбедени во деловната област
4) Управување со средства
5) Развој, набавка и одржување на информациски системи, вклучително мапирање на деловни процеси и придружна програмска логика
6) Управување со ИТ операции
7) Управување во физичко опкружување
8) Управување со човечки ресурси
9) Управување со комуникации
10) Управување со информациска безбедност[8]
11) Управување на усогласеност со закони
12) Управување со деловен континуитет и поврат од катастрофи
13) Управување со апликациски контроли

5.4 ВРИ можат да изберат временски период за ревизорска анализа (на пример една година, три години, итн.) при дефинирање на опфатот на ангажманот за ревизија на ИС. Може да се избере соодветен временски период кој е важен за дефинираните цели на ревизорскиот ангажман.

5.5 Кога ревизијата на ИС е дел од ревизорски ангажман, ВРИ може да се осигури дека ревизорскиот тим како целина работи на интегриран начин за да се постигне главната цел на ревизијата. За да се постигне ефективна интеграција, ВРИ може да размислат за:

1) Сеопфатно документирање на работата која треба да се изврши од ревизорите на ИС;
2) Дефинирање протокол за споделување на информации помеѓу ревизорите на ИС и другите ревизори;
3) Идентификување кои информациски системи и контролни цели се во рамките на опфатот на ревизијата;

5.6 ВРИ може да осигурат дека ревизорскиот тим е составен од членови кои заедно се компетентни да спроведат ангажмани за ревизија на ИС со цел да се постигнат предвидените ревизорски цели.

5.7 Потребното знаење, вештини и компетентност може да се стекнат преку комбинација на обука, регрутирање и ангажирање на надворешни ресурси, согласно стратешкиот план на ВРИ.

[7] Вклучително аспекти на стратешко управување

[8] Вклучително сајбер безбедност

5.8 Потребното знаење, вештини и компетентност може да се стекнат преку комбинација на обука, регрутирање и ангажирање на надворешни ресурси, според стратешкиот план на ВРИ.

5.9 ВРИ може да осигурат дека тимовите за ревизија на ИС заедно имаат капацитет:

1) Да ги разберат техничките елементи на еден ИТ-управуван информациски систем, вклучително сите релевантни примери на апликации во употреба, за да може да се пристапи и да се користи ИТ инфраструктурата за ревизорскиот процес
2) Да ги разберат постојните правила, регулативи и околината во која ИТ-управуваните информациски системи на субјектот работат
3) Да го разберат мапирањето на деловните процеси во програмската логика за информацискиот систем на субјектот на ревизија
4) Да применат и деловно и ИТ знаење за оценка на ризикот од рачно надминување на системската програма или конфигурација што ќе овозможи исклучителна обработка на трансакции
5) Да го оценат дизајнот и да ја тестираат ефикасноста на работењето на апликациските контроли во релевантните информациски системи
6) Да ја разберат ревизорската методологија, вклучително и релевантните ревизорски стандарди и упатства што се применуваат од страна на ВРИ
7) Да ги разберат ИТ критериумите за перформанс / усогласеност во однос на кои треба да се споредат наодите од ревизијата, вклучително и рамките за управување со ИС, како што се COBIT, ITIL, TOGAF
8) Да ги разберат техниките на ИС за собирање ревизорски докази од автоматизирани системи
9) Да ги разберат алатките за ревизија на ИС за собирање, анализа и репродукција на резултатите од таквата анализа или повторно извршување на ревидираните функции
10) Да пристапат и да ја употребат инфраструктурата на ИС за наоѓање и обезбедување на ревизорските докази
11) Да пристапат и да користат алатки за ревизија на ИС за анализа на собраните докази.

5.10 ВРИ може да разгледаат различни опции за алоцирање на човечки ресурси за ангажмани за ревизија на ИС. Ова може да подразбира воспоставување

на централна единица со ИТ специјалисти кои им помагаат на другите ревизорски тимови во ВРИ во спроведувањето на овие ревизии или да распоредуваат ИТ специјалисти на барање. Бидејќи бројот на преземени ангажмани за ревизија на ИС се зголемува, ВРИ може да размислат за формирање на посебна група или функција за ревизија на ИС. На оваа група може да и биде доверена одговорноста за спроведување на сите ангажмани за ревизија на ИС за ВРИ и да комуницираат со други тимови во ВРИ кои имаат претходно познавање на субјектот на ревизија, со цел брзо да добијат разбирање за функциите на ентитетот и поврзаните деловни процеси . Бидејќи технологијата сè повеќе се вметнува во информациските системи, ВРИ може да осигурат сите ревизори да се стекнат со соодветни вештини за ревизија на ИС.

5.11 ВРИ можат да ангажираат надворешни ресурси, како на пример ИТ консултанти, договорни изведувачи, специјалисти и експерти за спроведување на ревизија на ИС, во случај на ограничени ресурсите. ВРИ може да осигурат дека таквите надворешни ресурси се соодветно обучени и сензибилизирани за насоките за професионално однесување и за процесите и производите на ревизијата на ИС што се применуваат на ВРИ, и дека нивната работа е соодветно следена преку документиран договор или договор за ниво на услуга, како и соодветна вклученост на вработените на ВРИ во фазите на планирање, извршување, известување и следење на препораките на ревизијата. Затоа на ВРИ може да им бидат потребни квалификувани и со познавања членови на тимот во институцијата за да ја следат работата на надворешните ресурси и да го спроведат придржувањето кон упатствата и договорите за ниво на услуги.

5.12 За извршување на проценка на ризик во ангажмани за ревизија на ИС, ревизорите може да ги користат принципите утврдени во ISSAI 100, 200, 300 и 400 покрај оние што се користат за спроведување на одредена тема на ревизијата на ИС, како што е наведено подолу:

1) Инхерентен ризик се состои од веројатност дека одредени карактеристики на ИТ-управуваните информациски системи на ревидираниот субјект, по својата природа, може да резултираат во негативно влијание врз испораката на функцијата наложена да ја спроведува субјектот. На пример, информацискиот систем на субјектот на ревизија од кој се бара да ги направи достапни информациите за сите членови на јавноста, носи инхерентен ризик за изведба дека над предвидената горна граница на корисниците, информацискиот систем може да не реагира и информациите да не бидат достапни на било кој корисник. Иако субјектот на ревизија може да донесе контроли за ублажување на инхерентните ризици, во многу случаи субјектот можеби ќе мора едноставно да го толерира постоењето на таквите ризици во рамки на прифатливо ниво на ризици. Инхерентниот ризик може да се процени пред влијанието на контролниот ризик или ризикот на детекција да биде разгледано од ревизорите.

2) Контролниот ризик за ИС се состои од веројатноста дека ИТ контролите што биле донесени од страна на субјектот на ревизија не успеале да го ублажат негативното влијание за кое биле дизајнирани како одговор. На пример, информацискиот систем на субјектот на ревизија од кој се бара да осигури дека пристапот до доверливи податоци е ограничен само на овластен персонал, може да донесе контрола со барање за најавување со корисничко име и лозинка од страна на персоналот што се обидува да добие пристап. Контролниот ризик во оваа ситуација е корисничкото име и лозинката да не се соодветно безбедни и да можат да се претпостават од неовластен персонал преку повеќекратни обиди, што резултира во губење на доверливоста и потенцијално негативно влијание врз субјектот. Субјектот кој инсистира на употреба на безбедни, не тривијални лозинки кои содржат комбинација од букви, броеви и специјални симболи и кој гарантира дека информацискиот систем спречува пристап до корисничко име над одреден број на неуспешни обиди за добивање пристап, ќе има помал контролен ризик од оној што ги нема овие карактеристики.

3) Ризикот за детекција (откривање) се состои од веројатноста дека отсуството, неуспехот или несоодветноста на ИТ контролите донесени од субјектот, кои може да имаат потенцијално негативно влијание врз субјектот, да не бидат откриени од ревизорот.

5.13 За извршување на проценки засновани на ризик на ИТ управувани системи, ВРИ можат да изберат методологија која е соодветна за нивната намена. Таквите методологии може да се движат од едноставни класификации на профилот на ризик на ИТ околината на субјектот на ревизија како висок, среден и низок, врз основа на разбирањето на ВРИ за субјектот и неговата околина и професионалното расудување на тимот за ревизија на ИС на ВРИ, до посложени и нумерички пресметки кои го вбројуваат рејтингот на ризикот заснован на објективни податоци собрани од субјектот на ревизија[9].

5.14 Материјалноста на ревизијата на ИС може да се одреди според целокупната рамка за одредување за материјалноста во ВРИ. Перспективата на материјалноста може да варира во зависност од природата на ангажманот за ревизија на ИС. Материјалноста на финансиската ревизија, ревизијата на успешност и ревизијата на усогласеност, во кои е вклучен ангажманот за ревизија на ИС, се опишани во ISSAI 100, 200, 300 и 400[10].

[9] WGITA IDI Прирачник за ИТ ревизија за врховни ревизорски институции

[10] ISSAI 200 Принципи на финансиска ревизија, ISSAI 300Принципи на ревизија на успешност, ISSAI 400 Принципи на ревизија на усогласеност

6

Извршување на ревизија на информациски систем (ИС)

6.1 ВРИ можат да вршат ревизии на ИС во согласност со процесот опишан за ангажмани за финансиска ревизија (ISSAI 200), ревизија на успешност (ISSAI 300) и ревизија на усогласеност (ISSAI 400), во зависност од случајот, врз основа на природата на ангажманот.

6.2 Специфично за ревизија на ИС, ревизорите можат да побараат соодветна соработка и поддршка од субјектот на ревизија за завршување на ревизијата, вклучително пристап до записи и информации. Ревизорите може да идентификуваат начин на пристап до електронски податоци во формат неопходен за да се овозможи анализа, во консултација со субјектот на ревизија. Начинот на пристап до податоците би бил специфичен за ВРИ.

6.3 Пред да се започне со проценка на контролите во информацискиот систем, ревизорите може да се здобијат со разбирање на архитектурата на системот и основните податоци и нивните извори, со цел да ги идентификуваат потребните ревизорски алатки и техники.

6.4 Во случај на прием на префрлена голема количина на податоци[11] од субјектот на ревизија, ревизорите може да осигурат дека секоја префрлена голема количина на податоци е придружена со писмо од субјектот на ревизија. Таквото пропратно писмо може да го прецизира следното:

1) Изворот на податоците (преку упатување на временскиот печат генериран при префрлањето на податоците / хаш број за префрлање на податоци) за обезбедување интегритет на податоците, проверка на автентичноста[12] и непобивање[13].

2) Параметрите за екстракција користени за креирање на префрлена голема количина на податоци, на пр. користени пребарувања (queries) / стартувани извештаи.

3) Доколку такво пропратно писмо не е примено од субјектот на ревизија, може да се генерираат интерни документи од ревизорите во кои ќе бидат наведени важни информации, како на пр. датумот на предавање на податоците, од која датотека е креирано префрлањето на податоци, и дали

[11] Data dumps - Префрлени податоци се дефинирани како голема количина на податоци пренесени од еден систем или локација на друга

[12] Автентикацијата е дефинирана како акт за проверка на идентитетот на корисникот - Поимник на условите на ISACA

[13] Непобивањето се дефинира како уверување дека страната подоцна не може да го негира потеклото на податоците; обезбедување доказ за интегритетот и потеклото на податоците кои може да се проверат и од трето лице - Речник на термини на ISACA

податоците се од продукциска околина или од некоја друга околина итн.

6.5 Ревизорите можат да извршат проценка на ИТ контролите (општите и апликациските контроли) донесени од субјектот на ревизија, со цел да се испита нивната веродостојност и доволност. Проценката може да се изврши со употреба на соодветна комбинација на следниве техники: интервју, прашалник, набљудување, истражување на чекорите на процесот, дијаграм на проток на работа (flow chart), собирање и анализа на податоци, верификација, повторна пресметка, обработка и потврда од трета страна. Опфатот на проценката на ИТ контролите може да вклучи испитување за да се утврди дали:

1) Политика за ИС е дефинирана, усвоена и соопштена
2) Структурата за управување на ИС е воспоставена и функционална
3) Попис на средствата на ИС се врши периодично и се идентификуваат барања за зголемување, замена и отстранување на истите
4) Воспоставени се и функционални процеси за споделување на инфраструктура и заеднички услуги за ИС со други јавни субјекти
5) Дефинирани, усвоени и соопштени се процеси за развој, набавка и одржување на информациски системи (вклучително и оној за управување со промени)
6) Дефинирани, усвоени и соопштени се процеси за ИТ операции (внатрешни ресурси, надворешни ресурси, договор за услуги)
7) Донесени се мерки за осигурување физичка безбедност и предвидени се физички услови за работа
8) Донесени се мерки за обука и одговорност на човечките ресурси за осигурување доверливост, интегритет и достапност на информациите, како и усогласеност со барањата на политиката и структурата за управување со ИС
9) Донесени се мерки за осигурување доверливост, интегритет и достапност на различните начини и канали на комуникација
10) Донесени се мерки за управување со безбедноста на информациите
11) Донесени се мерки за управување со законската усогласеност
12) Донесени се мерки за континуитет на деловното работење и управување со поврат од катастрофи
13) Апликациските контроли донесени во рамките на секој информациски систем се соодветни и сигурни. Проценката на овие контроли може да вклучува идентификување на значајни компоненти на апликацијата, идентификување на критичката важност на апликацијата за субјектот, преглед на достапната документација, интервју со вработени,

разбирање на ризиците за апликациските контроли и нивното влијание врз субјектот, како и развој на тестови за да се испита соодветноста и веродостојноста на ваквите апликациски контроли.

6.6 Според тоа, проценката на општите и апликациските контроли, може да ги вклучува политиките, процесите, луѓето и системите на субјектот на ревизија, во согласност со целите на ревизијата на ИС.

6.7 Во зависност од целта на ревизијата, ревизорите може да се фокусираат на дизајнот, имплементација и ефикасноста на работењето на контролите. Кога ревизорот врши проценка на дизајнот на контролата, може да биде доволно интервју или проверка на документирани деловни правила. Кога ревизорот врши проценка на имплементацијата на контролите, може да не е доволно да се изврши само проверка, туку да биде потребно да се спроведе анализа на контролата чекор по чекор или да се изврши анализа на податоци за да се потврди дека контролата е имплементирана како што е дизајнирана. Ако, пак, ревизорот врши проценка на оперативната ефективност на контролата, од него/неа може да се побара да тестира примерок од трансакции за да демонстрира дека контролата работела ефективно во соодветниот период.

6.8 Ревизорите, исто така, може да вршат проценка како доказите за општите контроли влијаат на природата, времето и обемот на доказите потребни за да се добие уверување за работата на апликациските контроли. Доколку ревизорот има обезбедено доволни и соодветни ревизорски докази за ефективноста на општите контроли кои го поддржуваат логичкиот пристап на вработените до ИТ системите и управувањето со промените во продукциската средина, тој/таа може да изведе заклучок за оперативната ефикасност на автоматизираните процедури на апликациските контроли. Ова може да се постигне со тестирање на помал примерок на трансакции, бидејќи ефективноста на општото ИТ опкружување му обезбедува на ревизорот доказ за ефективноста на апликациската контрола во соодветниот период. Во случај на мануелни процедури на апликациските контроли, ревизорите може ќе треба да тестираат поголем примерок што одговара на избраното ниво на доверба.

6.9 Врз основа на проценката на ИТ контролите, ревизорите можат да ги идентификуваат приоритетни области за извршување на детално тестирање, кое вклучува детално тестирање на ИТ контролите со употреба на разни компјутерски потпомогнати ревизорски техники (CAAT's) за испитување, екстракција и анализа на податоци. Ревизорите може да дизајнираат и извршат детално тестирање со цел да ги потврдат целите на ревизијата. Ревизорите можат да изберат соодветни CAAT's во зависност од на нивните барања.

6.10 Ревизорите можат да користат разни CAAT's за ревизија на ИС како, на пример, анализа на дневник на корисници (кориснички логови), известување за исклучоци, проверка на збирови (тотали), споредба на датотеки, стратификација, избор на примерок, проверка на дупли записи, откривање на празнини во налозите, старосна структура на податоците, додавање и пресметки на виртуелно поле итн. Предностите на употребата на CAAT's вклучуваат анализа на големи количини на податоци, повторливост на тестовите на различни множества на податоци и со различни критериуми, како и генерирање документација за ревизорските тестови и добиените резултатите со време на реализација.

6.11 Ревизорите може секогаш да не бидат во можност да ги испитаат сите случаи, трансакции или модули или ИТ системи, со оглед на ограничувањата на ресурсите и компромисот на трошоците и придобивките во текот на ревизијата. Во таков случај, ВРИ може, врз основа на утврдената материјалност, да одреди избор на примерок за детално испитување за да се извлечат разумни ревизорски заклучоци. ВРИ може да користат соодветни CAAT's за вршење различни видови на избор на примерок и да ја утврдат соодветна големина на примерокот во зависност од основните инхерентни и контролни ризици. Изборот на ревизорски примероци[14] се врши со цел на ревизорот да му обезбедат разумна основа за изведување заклучоци за целата популација на податоци, а врз основа на заклучоци добиени со примената на ревизорските процедури и анализа на ревизорскиот примерок. Ревизорите може да ја земат во предвид целта на ревизорскиот процес и карактеристиките на популацијата од која се врши изборот на примерок за да ја одредат соодветната големина на примерокот за да се намали ризикот на примерокот на прифатливо ниво. Ревизијата во ИТ околина може да помогне во анализа на 100 проценти од популацијата, особено во фазата на прелиминарното истражување. Сепак, за детално тестирање може да биде потребно да се изврши избор на примерок. Кога се врши избор на примерок во рамки на финансиска ревизија, ИТ ревизорите можат да го применат ISSAI 2530[15].

6.12 Ревизорите можат да осигурат дека собраните и документирани електронски докази се доволни, сигурни и точни за прифаќање на заклучоците на ревизијата. Вакви електронски докази може да бидат датотеки со податоци, дневници на корисници (кориснички логови), аналитички модели, извештаи за

[14] ISSAI 2530, *Финансиска ревизија, Избор на примерок во ревизијата*, точка 6 до 9

[15] ISSAI 2530, *Финансиска ревизија, Избор на примерок во ревизијата*, точка 6 до 9.

управување со информациски системи итн., а тие може соодветно да се соберат и складираат на начин да бидат достапни за да се обезбеди уверување за точноста и валидност на ревизорскиот процес. Доказите собрани за време на ревизијата на ИС може да имаат временски ознаки (време на обезбедување на податокот) и детали кои ги содржат чекорите на извршување на анализата на податоците, така што јасно ќе се знае кога доказите биле креирани, складирани и последен пат изменети, за да се намали ризикот од последователни промени.

6.13 Документацијата за ревизија на ИС може да се зачува и заштити од какви било измени и неовластено бришење. ВРИ можат да развијат нови стандарди за чување на документацијата за ревизија на ИС или да ги прилагодат постојните стандарди за да ги исполнат барањата за чување на документација од ревизија на ИС. Така достигнатиот периодот на чување на документацијата, ќе биде функција на мандатот на секоја ВРИ и статутот (ите) што ги регулира нивните активности. Посебно внимание може да се посвети на медиумите, форматот, очекуваниот век на траење и барањата за складирање на овие податоци, за да се осигури дека податоците може да се читаат во временската рамка дефинирана во политиката за чувување и архивирање на податоците на секоја ВРИ. Ова може да бара претворање на податоците од еден во друг формат за да се држи чекор со технолошкиот напредок и застареноста.

6.14 Во случај на испитување на технички извештаи изготвени од трети лица - ревизори за специфични теми од областа на технологијата, ревизорите можат да усвојат соодветни процедури, за да добијат уверување за усогласеноста, финансиските аспекти или изведбата (перформансот) на овие извештаи[16]. Ако, како резултат на процедурите, се потпрат на содржината на таквите извештаи, фактот за потпирање на истите може соодветно да се обелодени.

6.15 ISSAI пропишуваат дека ревизорите треба да воспостават ефективна комуникација во текот на целиот процес на ревизија и да го информираат субјектот на ревизија за сите прашања поврзани со ревизијата (сп. ISSAI 100, параграф 43). Во ревизиите, кои вклучуваат и ревизија на ИС, резултатот од ИТ ревизијата, во некои случаи може да му се соопшти на субјектот со посебно писмо. Во овие случаи, може да е важно да се објасни како резултатот од ревизорската работа е поврзана со останатата комуникација која е дел од истата финансиска ревизија, ревизија на успешност или усогласеност, и како резултатите од работата на ревизијата на информациските системи може да бидат релевантни за извештајот на ВРИ од извршената ревизија.

[16] Кога опфатот е во рамките финансиска ревизија, ревизорите може да го користат ISSAI 2402 *Ревизорски разгледувања во врска со ентитети кои користат услужни организации*

7

ИЗВЕСТУВАЊЕ ЗА РЕВИЗИЈА НА ИС

7.1 Со оглед на тоа што ангажманот за ревизија на ИС претставува финансиска ревизија (ISSAI 200), ревизија на успешност (ISSAI 300) или ревизија на усогласеност (ISSAI 400), ревизорите можат соодветно да ги разгледаат барањата за известување. Ова е специфично за секоја ВРИ. Слично на тоа, секоја ВРИ може да има свои прагови за известување засновани врз материјалноста на наодите од ревизијата. Слично на тоа, ревизорот, кога известува за ревизија на ИС, може да ги земе предвид законските и интерните ограничувања за откривање на финансиски и технички информации.

7.2 Ревизорите може да ја согледаат потребата од ограничување на употребата на технички жаргон, и чувствителноста на презентираните информации (на пр. лозинки, кориснички имиња, лична карта и лични информации) во извештајот. И покрај техничката природа на ревизијата на ИС, ревизорите може да осигурат дека извештајот е целосно разбирлив за високото раководство на субјектот на ревизија, засегнатите страни и поширокаата јавност. Во извештаите, ревизорите можат да вметнат соодветно детален поимник на термини кои упатуваат на дефиниција на кратенка или термин, со објаснување засновано на случаи како тоа работи во контролирана средина.

7.3 Ревизорите може да го земат во предвид потенцијалното негативно влијание на извештајот од ревизијата на ИС по неговото објавување. На пример, ако извештајот за ревизија на ИС открива некои безбедносни ризици во информацискиот систем на субјектот на ревизија и истите се објават пред да бидат донесени неопходни контроли за намалување на ризиците, ранливоста на информацискиот систем на субјектот може да биде достапна на јавноста. Во таков случај, ревизорите можат да разгледаат опции како, на пример, објавување на извештајот по донесување на потребните контроли или да не се известува за конкретен безбедносен ризик во целост, со цел да се избегне потенцијално негативно влијание врз ревидираниот субјект.

8

FOLLOW UP

8.1 Кога ангажманот за ревизија на информациски системи произлегува од еден или повеќе од главните видови на ревизија, ревизорите може да ги земат во предвид барањата за следење (follow up) на таквите ревизорски ангажмани кои се во согласност со оние за финансиска ревизија (ISSAI 200), ревизија на успешност (ISSAI 300) и ревизија на усогласеност (ISSAI 400).